interweb

Gerado a 15/11/2026 00:29

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Ataque DDoS ou apenas um pico de visitas: como distinguir, e o que fazer

Avisos de abuso e listas negras

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1492	v2026.10.18	Angola · Português

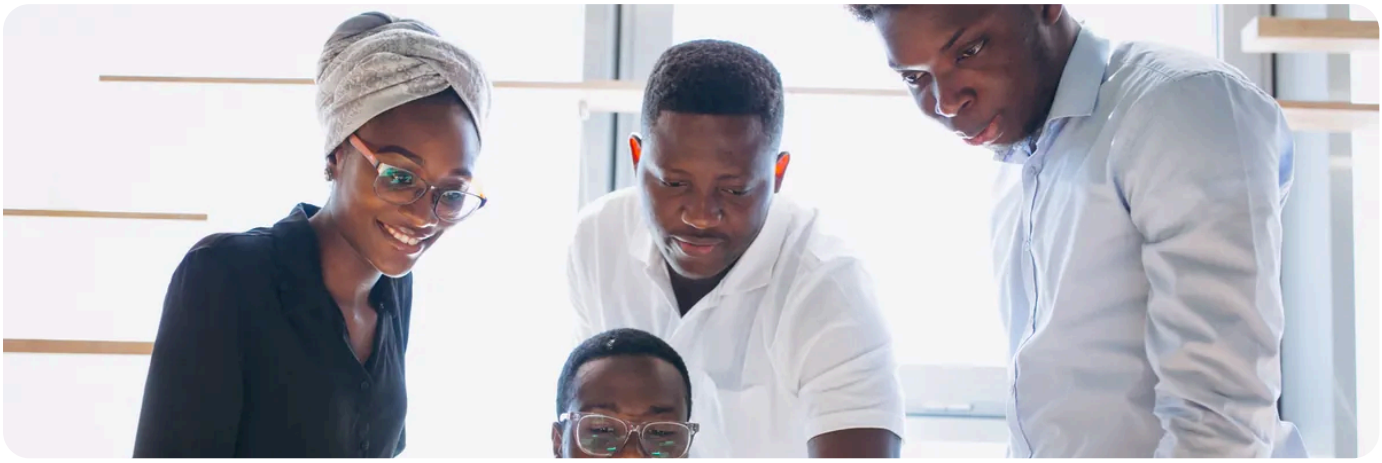
Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1492

Ataque DDoS ou apenas um pico de visitas: como distinguir, e o que fazer

Avisos de abuso e listas negras · Criado em **10 de outubro de 2026** · Atualizado em **18 de outubro de 2026**

4 min de leitura



A resposta curta: um ataque **DDoS** (negação de serviço distribuída) é uma inundação de pedidos falsos, vindos de muitos endereços ao mesmo tempo, para que o site deixe de responder aos pedidos verdadeiros. Mas a maior parte dos «ataques» que os clientes nos reportam são outra coisa: **uma campanha que correu bem**, **robôs a ler o site todo** ou **um *plugin* a pedir demasiado**. A diferença percebe-se olhando para *quem* está a pedir e *o quê*.

As quatro explicações mais comuns

Causa	Como se parece	O que fazer
Pico real de visitas	Subida logo a seguir a uma publicação, a um anúncio ou a uma menção na imprensa. Os visitantes veem páginas diferentes e passam algum tempo no site.	Nada de hostil: é bom sinal. Se o site aguenta mal, veja **o que realmente faz diferença na velocidade**.
Robôs e rastreadores	Muitos pedidos, de endereços de poucas origens, a percorrer todas as páginas ou as pesquisas internas.	Limitar com `robots.txt` e bloquear os piores. Veja **robôs de IA a ler o seu site**.
Um *plugin* ou script a pedir demasiado	O consumo de recursos sobe sem subir o número de visitantes. É típico de `admin-ajax.php` ou de uma tarefa agendada.	Veja **o admin-ajax a gastar recursos**.
Ataque verdadeiro	Milhares de pedidos por minuto, de muitos endereços sem relação, quase todos ao mesmo endereço: a página de entrada, a pesquisa, o `wp-login.php`, o `xmlrpc.php`. As páginas pedidas não variam e ninguém fica no site.	Ver abaixo.

Como confirmar, em quatro passos

1. **Anote a hora do início** e como começou: de repente, ou em rampa.

2. **Veja as estatísticas no cPanel** (os visitantes e os acessos brutos). Os endereços e as páginas mais pedidas dizem muito. Veja onde estão em **as estatísticas de visitantes**.

3. **Veja os erros que o site devolve.** Um erro 508 ou 503 quer dizer que o site chegou aos limites da conta ou que o servidor está ocupado: **erros do site: 500, 403, 404 e 508**.

4. **Compare com um dia normal.** Se a atividade só mudou numa página ou num endereço, é quase sempre o site; se mudou em tudo e a partir de todo o lado, é provável que seja externa.

Se for um ataque

1. **Fale connosco logo.** Os nossos servidores têm filtragem de ataques volumétricos ao nível da rede, e vemos o que chega ao servidor. Diga-nos a hora de início e o domínio atingido. O que fazemos e o que continua a ser seu está em **o que fazemos pela segurança, DDoS incluído**.

2. **Se os endereços são poucos e claros,** bloqueie-os, como em **bloquear um IP de visitar o seu site**. Num ataque a sério são demasiados para isso.

3. **Se o seu site é um alvo provável,** ponha-o atrás de um serviço que filtre os pedidos antes de chegarem ao servidor, com um «modo de emergência». O Cloudflare é um exemplo, e é uma conta sua. Veja **quando ajuda e como ligar**. Nenhum serviço promete proteção absoluta.

Mensagens que exigem dinheiro para não atacar o site

são, quase sempre, só a mensagem: ameaçam um ataque que ainda não começou. Não pague, não responda e guarde o e-mail. Num ataque muito grande, a solução habitual da rede é desligar o tráfego ao endereço atingido durante umas horas: desagradável, e é a menos má das opções.

Deixar o «modo de ataque» de um serviço de proteção ligado para sempre faz cada visitante passar por uma verificação antes de ver o site. Ligue-o durante o ataque e desligue-o depois.

PRECISA DE AJUDA?

O site ficou lento ou deixou de responder e suspeita de um ataque? Diga-nos a hora e o domínio.

Abrir pedido de suporte →

Onde ver na sua conta

- **Uso de recursos** (Resource Usage) no cPanel: gráficos de CPU, memória, I/O e processos de entrada contra os limites da sua conta, com os momentos em que um limite foi atingido. Uma inundação de pedidos aparece como uma subida repentina que toca no tecto.
- **Erros 508 ou 503** ao visitar o site: o 508 quer dizer que a conta chegou aos limites, o 503 que o servidor estava ocupado.
- **Estatísticas de visitantes e registo de acessos em bruto**, em Metrics: os endereços e as páginas mais pedidos nessa altura.

Leve esses três ao pedido de suporte, com a hora de início, o domínio e, se puder, uma captura do Uso de recursos. Com isso conseguimos dizer muito mais depressa se a causa é o site ou algo de fora.

VEJA TAMBÉM

- **O que fazemos pela segurança, DDoS incluído, e o que fica por sua conta**
- **Bloquear um IP de visitar o seu site**
- **Robôs de IA a ler o seu site: robots.txt e como os bloquear**
- **Cloudflare: quando ajuda e como ligar**

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-1492 · v2026.10.18 · Gerado a 15/11/2026 00:29